

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 defining a key and a set of values, the key being
3 determined by the values and a predefined relationship,
4 sending one of the values of the set and information
5 encrypted using the key to a server; and
6 sending another of the values of the set to a first
7 delegate.

1 2. The method of claim 1 further comprising:
2 generating a second set of values, the key being
3 also determined by the values of the second set;
4 sending one of the values of the second set to the
5 server; and
6 sending another of the values of the second set to a
7 second delegate.

1 3. The method of claim 2 in which the values of the
2 second set are also determined by the predefined relationship.

1 4. The method of claim 1 in which the set includes
2 exactly two values.

1 5. The method of claim 1 in which the set includes three
2 or more values.

1 6. The method of claim 1 in which the value of the set
2 sent to the server is associated with a descriptor of the
3 first delegate.

1 7. The method of claim 1 in which the probability of
2 guessing the key correctly using knowledge of one or more of
3 the values of the set, but not all the values of the set is
4 the same as the probability of guessing the key correctly
5 using no knowledge of any value of the set.

1 8. The method of claim 7 in which the predefined
2 relationship comprises the Boolean XOR function or a
3 relationship that applies an encryption algorithm to one value
4 of the set using another value of the set as the encryption
5 algorithm key.

1 9. The method of claim 1 in which the information
2 comprises medical information.

1 10. A method comprising:
2 storing, on a server accessible through a network,
3 secured information and a first access component, use of the
4 secured information requiring the first access component and a
5 second access component; and
6 providing the secured information and the first
7 access component to a first requestor.

1 11. The method of claim 10 in which the second access
2 component is not stored on the server.

1 12. The method of claim 10 further comprising storing a
2 third access component, such that the third access component
3 and a fourth access component are sufficient to permit use of
4 the secured information.

1 13. The method of claim 12 further comprising providing
2 the secured information and the third access component to a
3 second requestor.

1 14. The method of claim 12 further comprising deleting
2 the third access component in response to a trigger, the
3 trigger being a client instruction, a time limit, a request
4 from the first requestor, or a security breach.

1 15. The method of claim 12 further comprising
2 identifying the requestor and determining that the requestor
3 requires the first access component but not the third access
4 component.

1 16. The method of claim 10 further comprising storing
2 permission information about the identity of a party approved
3 for access, such that the secured information and the first
4 access component are only provided if the first requestor is
5 an approved party.

1 17. The method of claim 10 in which the secured
2 information is secured by encryption using a key, and the
3 first and second access components are related to the key by a
4 predefined relationship.

1 18. A method comprising:
2 receiving
3 a) from a client, a first access component
4 required for use of secured information, the use requiring the
5 first access component and a second access component,
6 b) from a server accessible through a network,
7 the secured information, and
8 c) from a source other than the client, the
9 second access component.

1 19. The method of claim 18 in which the source is the
2 server.

1 20. The method of claim 18 in which the source is other
2 than the server.

1 21. The method of claim 18 in which a third access
2 component is required in addition to the first and second
3 access components for use of the secured information.

1 22. The method of claim 18 in which the secured
2 information, the first access component, and the second access
3 component are received in a digital form.

1 23. An article comprising a machine-readable medium that
2 stores machine-executable instructions, the instructions
3 causing a machine to:

4 define a key and a set of values, the key being
5 determined by the values and a predefined relationship,
6 send one of the values of the set and information
7 encrypted using the key to a server; and
8 send another of the values of the set to a first
9 delegate.

1 24. The article of claim 23 in which the instructions
2 further cause a machine to:

3 generate a second set of values, the key being
4 independently determined by the values of the second set;
5 send one of the values of the second set to the
6 server; and
7 send another of the values of the second set to a
8 second delegate.

1 25. An apparatus comprising a processor and instructions
2 configured to cause the processor to:

3 receive, from a client, information and a value of a
4 set of values, the information being encrypted using a key,
5 the key being determined by the values of the set and a
6 predefined relationship;

7 store the information and the value, but not all the
8 values of the set; and

9 transmit, to a delegate, the information and the
10 value.

1 26. The apparatus of claim 25 in which the software is
2 further configured to cause the processor to:

3 store a second value that is a member of a second
4 set of values, the values of the second set being sufficient
5 to determine the key using the predefined relationship.

1 27. The apparatus of claim 25 in which the software is
2 further configured to cause the processor to:

3 delete or deny access to the second value in
4 response to a trigger, the trigger being a client instruction,
5 a time limit, a request from the delegate, or a security
6 breach.

1 28. The apparatus of claim 25 in which the information
2 comprises medical information.

1 29. A method comprising:
2 encrypting information using an encryption key;
3 sending the encryption key, but not the encrypted
4 information to a first party;
5 sending the encrypted information, but not the
6 encryption key to a server.

1 30. The method of claim 29 further comprising sending a
2 descriptor of the first party to the server to thereby
3 authorize the server to provide the encrypted information to
4 the first party.